**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF VIRGINIA**
**(ALEXANDRIA DIVISION)**

| | | |
|---|---|---|
| **GLOBAL POLICY PARTNERS, LLC *et al.*,** | ) | |
| **Plaintiffs,** | ) | **Case No. 1:09CV859 TSE-TRJ** |
| **v.** | ) | |
| **BRENT YESSIN *et al.*,** | ) | |
| **Defendants.** | ) | |

**PLAINTIFFS' OBJECTIONS TO THE MAGISTRATE JUDGE'S DECEMBER 23, 2009 ORDER DENYING PLAINTIFFS' SECOND MOTION TO COMPEL**

Pursuant to Fed. R. Civ. P. 72(a), Plaintiffs Global Policy Partners, LLC ("GPP") and Katherine Friess ("Ms. Friess") (collectively, "Plaintiffs"), by and through their undersigned counsel of record, respectfully submit their Objections to the Magistrate Judge's December 23, 2009 Order denying Plaintiffs' Second Motion to Compel Inspection of Defendant Yessin's Computer Hard Drive.

## I. INTRODUCTION

Plaintiffs' claims against Defendant are based on the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") (Counts I-II) and the Stored Wire and Electronic Communications and Transactional Records Act, 18 U.S.C. § 2701 *et seq*. (Counts VI-VII) (the "Stored Communications Act" or the "SCA"). As demonstrated below, since the inception of this matter, Plaintiffs have diligently sought an imaged-copy of Defendant's hard-drive in order to establish his liability and the extent of Plaintiffs' damages under the SCA and the CFAA. In order to do so, Plaintiffs have submitted

numerous briefs and Declarations from their forensic computer expert and cited numerous cases from this jurisdiction and others which hold that in cases involving the same statutes at issue here, Plaintiffs are entitled to forensically analyze Defendant's hard-drive.

In response, Defendant has consistently argued that he should not have to produce his hard-drive because he is a practicing attorney and his attorney-client communications with others would be divulged. Defendant makes this claim even though he admits that he accessed at least four of Plaintiffs' email accounts, one such account for almost two years, and admittedly accessed and copied privileged emails relating to Ms. Friess' divorce and settlement strategy and shared these privileged communications with another attorney who was providing legal advice regarding his contested divorce with Ms. Friess. Defendant also admits that he accessed Plaintiffs' email accounts on many other occasions, but despite claiming to have a photographic memory, he allegedly cannot remember how many times he accessed those accounts, or what emails he viewed. In discovery, Defendant has only produced ***two*** email strings, which not coincidentally are the same emails referenced in the Amended Complaint. Thus, even though he unlawfully accessed Ms. Friess' attorney-client communications is using them against her in an on-going, contested divorce proceeding, Defendant contends that, unlike virtually every other case of this nature, he is not required to produce an imaged-copy of his computer so that Plaintiffs can establish how many times he accessed their accounts and what he did with this information.

What is even more galling is that at his deposition, and contrary to what he and his counsel have been representing to The Magistrate Judge, Defendant admitted under

oath that he has been "removed long enough from the daily practice of law" and refused to identify the name of a single client with whom he had an attorney-client privilege or relationship. When Plaintiffs' counsel pressed Defendant to provide this information to determine whether there was a privilege that would justify withholding the computer, his counsel instructed him not to answer the question. Defendant cannot continue to have it both ways – he cannot invoke the privilege to not produce his hard drive and then refuse to produce the most basic information in order to establish whether a privilege exists in the first place. Defendant's refusal to produce this information indicates that the premise for not producing an imaged-copy of his hard-drive, which was relied upon by the Magistrate Judge, simply was not true.

Defendant also has argued that Plaintiffs are not entitled to a complete forensic exam because Defendant's December 4, 2009 production allows Plaintiffs to "see whether any file that resided in the GPP email account assigned to Ms. Friess now resides on [Defendant's] computer." Defendant's Rebuttal at 2. Similarly, Defendant argues that Plaintiffs have not demonstrated that Defendant "copied anything more then what was already produced" *Id.* at 3. The glaring hole in these arguments is that they rely on the faulty premise that Defendant's liability – and Plaintiffs' discovery rights and damages – are limited to what Defendant ***copied*** from Plaintiffs' email accounts onto his computer. Liability under both the CFAA and SCA is premised on Defendant's unlawful access to Plaintiffs' email accounts, not on whether he ***copied*** emails onto his hard drive. Copying emails proves Defendant accessed Plaintiffs' email accounts on a number of occasions, but Defendant admittedly accessed Plaintiffs' accounts on numerous other occasions without copying an email communication to his hard drive. Defendant's

attempt to limit this case to only emails or documents he ***copied*** from Plaintiffs' email accounts (that he is willing to identify) defies the governing law and common sense.

In disregard of Plaintiffs' expert Declarations and the governing law, the Magistrate Judge denied Plaintiffs' repeated requests for an imaged-copy of Defendant's hard-drive. Instead, based upon Defendant's false representations about his attorney-client communications, the Magistrate Judge accepted Defendant's approach and only permitted Plaintiffs to have the results of "key-word" searches and the unallocated space on Defendant's hard-drive (which is a tiny fraction of the hard-drive). As Plaintiffs' expert Declarations make clear, this is entirely inadequate. First, under this approach, Plaintiffs were required to devise perfect key-work searches to obtain all responsive information. In order to do so, Plaintiffs would have to know what Defendant accessed and what he did with this information. Only Defendant possesses this information and he refuses to produce it. More importantly, Defendant was then permitted to vet the results of these searches for "responsiveness", so he alone could decide what Plaintiffs were entitled to see. Second, as Plaintiffs' expert Declarations make clear, the responses to the key word searches and the unallocated space of Defendant's hard-drive will not tell Plaintiffs how many times Defendant accessed their email accounts and what he did with this information, which is critical to Defendant's liability and Plaintiffs' damages.

Thus, although Defendant has admitted repeatedly accessing Plaintiffs' email accounts and sharing this information with third parties in order to harm Plaintiffs, the Magistrate Judge has permitted ***Defendant*** to provide Plaintiffs with the evidence of his unlawful conduct that he feels like producing, instead, as the governing law dictates, allowing Plaintiffs to discover this information through a forensic examination. This is

akin to allowing the fox to guard the henhouse and Defendant has taken full advantage of this approach – although he has admitted to accessing some of Plaintiffs' accounts for almost two years, he has produced only ***two*** email strings which happen to be the emails referenced in Plaintiffs' Amended Complaint. In other words, Defendant has only produced that which he knew Plaintiffs were already aware of and nothing more.

As Plaintiffs have repeatedly stated in the course of this litigation, they have no interest in any truly privileged communications existing on Defendant's hard drive – their only interests are determining how many times Defendant unlawfully accessed their email accounts and what Defendant did with this information. The only way to obtain this information is to conduct a complete forensic examination of Defendant's hard drive, not the truncated assortment of unallocated space and key word results that Plaintiffs have been permitted to review.

## II. PROCEDURAL HISTORY

From the very beginning of this litigation, Plaintiffs have been diligently seeking the production and forensic examination of Defendant's hard drive to determine how many times Defendant accessed Plaintiffs' email accounts and what he did with that information.

### A. Motion For Expedited Discovery

In August 2009, Plaintiffs initially prepared a Motion to Expedite Discovery to seek production of an imaged-copy of Defendant's computer even before discovery was permitted in this case. Before filing that motion, Plaintiffs' counsel met and conferred with Defendant's counsel, who agreed to immediately obtain an imaged-copy of Defendant's computer. Based on that representation, Plaintiffs agreed to hold-off filing

the Motion, however, Defendant refused to produce the imaged copy of the computer to Plaintiffs for a forensic analysis.

**B. The Initial Pre-Trial Conference And Plaintiffs' First Motion To Compel**

On October 7, 2009, the parties and the Court conferred pursuant to Fed. R. Civ. P.16(b). At the Conference, counsel for the Plaintiffs stated that among the discovery issues between the parties was Defendant's objection to producing his computer or an imaged copy of the computer's hard drive for forensic analysis by Plaintiffs' expert. The Magistrate Judge instructed Plaintiffs to file their Motion to Compel by Monday, October 12, with argument to be heard on October 16.

Pursuant to the Magistrate Judge's instructions, Plaintiffs filed their first Motion to Compel a forensic analysis of Defendant's computer hard drive on October 12, 2009. Plaintiffs consistently stressed that a forensic examination of Defendant's computer was necessary to determine both the extent of Defendant's liability and Plaintiffs' damages. In this Motion, Plaintiffs explained:

> A forensic analysis of Defendant's computer(s) will enable Plaintiffs to determine when, and how often, Defendant unlawfully accessed Plaintiffs' computer and email system, as well as which documents and emails Defendant reviewed, saved and shared with others. This will enable Plaintiffs to determine the full extent of Defendant's liability, as well as the full extent of Plaintiffs' damages.

(Ex. A at 1).

In the first Motion to Compel, Plaintiffs also cited cases similar to this one in which courts granted the forensic examination of a computer hard drive to preserve relevant information. In his Opposition (Ex. B), Defendant disingenuously argued that Plaintiffs were seeking unlimited access to communications between himself and his business clients and confidential communications between himself and his counsel

regarding this case, his pending divorce, and the Florida declaratory judgment action regarding management and control of GPP. (*Id.* at 8). Plaintiffs explained in their Reply (Ex. C), that contrary to Defendant's Opposition, Plaintiffs did not seek unfettered access to Defendant's personal, business, or privileged files on his computer, and that "their only interest is which of Plaintiffs' emails and documents Defendant accessed and reviewed, how he used them, and who he shared them with and for what purpose." (*Id.* at 2).

At the October 16 hearing, the Magistrate Judge instructed the parties to further meet and confer to ascertain whether the Defendant's production of certain files from his hard drive, as opposed to the actual computer or imaged hard drive copy, would suffice.

Accordingly, on October 19, the parties and their respective experts engaged in a joint conference call. At that point, Defendant's expert, Mr. Ben Pim, had not yet fully examined the hard drive of the Defendant, and could not answer many of the questions posed by Plaintiffs' computer forensic expert, Mr. Jason Sprowl. During that conversation, Defendant's expert also noted that the imaged copy of the hard drive, which Defendant had promised to have made over a month before, was copied incorrectly. Defendant's expert asked Plaintiffs' expert to e-mail him a list of the items that he would need in order to conduct a proper forensic analysis. Later that day, Plaintiffs' expert sent him such a list. On Wednesday, October 21, 2009, counsel for the Defendant responded by letter stating that the items enumerated by Plaintiffs' expert constituted essentially the entire hard drive. Counsel for the Defendant proposed, instead, that his expert conduct a "key word" search.

On October 22, and pursuant to the Magistrate Judge's instructions, the parties submitted supplemental briefing. Defendants argued in their supplemental brief that a

key word search of the files on the hard drive should be conducted. (Ex. D). Plaintiffs' supplemental brief included detailed Declarations from their forensic expert, Mr. Sprowl, explaining why data recovery efforts such as a key word search cannot substitute for a comprehensive forensic examination of Defendant's computer. (Ex. E, at 4-5). Plaintiffs also thoroughly addressed Defendants' privacy concerns, citing several cases in which the Courts permitted a plaintiff to conduct a ***full*** forensic examination of a defendant's computer after ensuring that the defendant first had the opportunity to review the materials to separate non-responsive and privileged documents. Plaintiffs proposed, in keeping with these cited cases, that "their expert agrees to a confidentiality agreement or Protective Order, performs the searches necessary in his expert opinion to reveal the relevant files, and then hands those files over to counsel for Defendant. Counsel then reviews the files for privilege, creates a privilege log, and produces the privilege log, along with all non-privileged, responsive documents." (*Id.* at 9).

The Court heard the final argument on Plaintiffs' first Motion to Compel on Friday, October 23. Over, Plaintiffs' objections, the Magistrate Judge decided to permit Defendant's key word search protocol to be implemented instead of permitting a forensic examination. The Magistrate Judge specifically recognized that the key word protocol could address, at best, the content of the emails Defendant accessed rather than the separate questions of when and how many times Defendant accessed Plaintiffs' email accounts:

> THE COURT: Well, what does your expert say he's going to do other than a key word search with respect to any area of the disk that's not occupied by a file? Is he going to look at every bit and byte individually as it streams across his screen? And what's he going to be looking for if not key words?

> MS. HARRIS: I believe that's part of it. But I believe he can also look at when the computer connected to a certain Web site.
>
> THE COURT: How does that relate to what we're talking about here?
>
> MS. HARRIS: Because it will show when he was on her e-mail account. And when he was on any GPP e-mail account. In addition, the allocated clusters, as my expert—
>
> THE COURT: ***That's a separate issue. You know, that's where we started, I guess. I'm going to have to come back to that. But right now we're talking about content and not instances of access.***

(Ex. F, at 16) (emphasis added).

> As for its decision to utilize a key word search only, the Court also noted that:
>
> THE COURT: ***I wouldn't be doing it this way if it weren't a hard drive on which a substantial amount of material is, covered by the attorney/client privilege is stored. But that's a fact that I have got to deal with***. There is no indication that that situation was brought into play as a shield of some sort, it's just the nature of this hard disk.

(*Id.* at 18, emphasis added). The Magistrate Judge made it abundantly clear that he was not permitting a forensic exam because of Defendant's representations that the hard drive contained attorney-client communications that had to be protected. As demonstrated below, these representations were not true. The Magistrate Judge also erred by focusing on the content of the material Defendant accessed instead of when and how many times Defendant accessed Plaintiffs' email accounts and what he did with this information. Finally, the Magistrate Judge made clear that his decision "is without prejudice to plaintiffs' ability to come back and ask for more if you have reason to believe you haven't gotten what you're entitled to." *Id.* Because the Magistrate Judge denied Plaintiffs' Motion without prejudice, Plaintiffs could not file Objections at that time.

**C. <u>Implementation of Protocol Order</u>**

While disagreeing with the Magistrate Judge's ruling, Plaintiffs did their best to quickly and timely comply with the key word search protocol order that the Court adopted. (Ex. G). Although Plaintiffs believed that the key word search would be insufficient to determine when and how many times Defendant accessed Plaintiff's email accounts, Plaintiffs understood they needed to permit the Magistrate Judge' key word search protocol to run its course prior to again moving to compel a complete forensic examination of Defendant's computer.

The implementation of the Court's key word protocol order was not without problems and delays. Plaintiffs' counsel worked extensively with Ms. Friess to create and narrow the initial list of key words terms and this process took time and many communications to finalize the key word list. Plaintiffs made a good faith effort to provide a comprehensive search list and submitted it to Defendant's counsel on November 3. Later, in the interest of trying to meet the Court's original expert deadlines, Plaintiffs eliminated some search terms to expedite the process.

In contrast to Plaintiffs' actions, Defendants delayed the process with mistakes and false starts. On November 16, Plaintiffs' counsel sent Defendant's counsel an email recounting the numerous mistakes Defendant had made in the search process, which resulted in delays. As Plaintiffs reminded Defendant:

> [D]efendant has caused some undue delay. We sent you the list of key terms on Nov. 3 and you agreed to them on Nov. 4. Paragraph 4 of the protocol order states: "Within 2 business days of reaching agreement on the search terms, Mr. Pim will implement a search of Defendant's hard drive using the search terms." Defendant could not run a search within this time period because they had not yet begun the indexing of the hard drive, a process that should have been done well in advance of when we sent you our key word list. The indexing was not completed until 5 days later on Nov. 9, three business days after we had reached agreement on the key word terms. We then lost an additional day on November 10, when

> defendant mistakenly used default word key lists and numbers such as "2" and "3", which slowed the search to a crawl and necessitated beginning the search all over again. Then on Nov. 11, a second search had to be run because Mr. Sprowl noticed that approximately 46 of our key words/terms were missing and had not been entered for processing in the forensic software. These delays have generated no less than two and half days of lost time.

(Ex. H).

Despite these delays, Defendant completed the key word search and provided the Plaintiffs the results on December 4. Defendant also produced an external hard drive containing the hard-drive's unallocated space, which Defendant provided because it could not separate privileged information from information containing key word hits in the unallocated space portion of the hard drive.

**D. Plaintiffs' Second Motion To Compel**

As anticipated, the key word search and the extraction of the unallocated space (which was only a very small portion of the hard-drive) did not provide Plaintiffs with the information necessary to determine when and how many times Defendant accessed their email accounts, which are critical questions for proving both the extent of liability and actual and statutory damages under the CFAA and SCA. As a result, on December 4, Plaintiffs promptly filed a Second Motion to Compel a forensic examination. (Ex. I). Defendant filed an Opposition Brief (Ex. J) and Plaintiffs filed a Reply (Ex. K). The Magistrate Judge heard argument on the Second Motion to Compel on December 11. (Ex. L). The Magistrate Judge then permitted Plaintiffs to file another expert Declaration on December 14 and canceled the December 14 due date for Plaintiffs' expert report. (*Id.* at 29).[1] Defendant then filed two Declarations from their experts and a rebuttal brief on

[1] The Magistrate Judge has not yet re-set the expert deadlines.

December 16. (Ex. M). Because Defendant went beyond the Court's request for additional Declarations and also submitted an extensive brief, the Magistrate Judge gave Plaintiffs leave to file a final rebuttal brief by December 21. (Ex. N).

During the briefing of the Second Motion to Compel, Plaintiffs' forensic expert submitted multiple Declarations to the Court, repeatedly explaining that the key word search results and unallocated space alone was wholly insufficient to determine when and how many times Defendant accessed Plaintiffs' email accounts and what he did with this information. On December 23, the Magistrate Judge issued an Order denying Plaintiffs' Second Motion to Compel because it found that "the information plaintiff [sic] seeks to discover could be obtained from the discovery already provided by defendants [sic]." (Ex. O).

Plaintiffs respectfully object to this Ruling.

## III. ARGUMENT

Under Fed. R. Civ. P. 72(a), a party may serve objections to a magistrate judge's non-dispositive order within 14 after being served with a copy. The district court must "modify or set aside any part of the order that is clearly erroneous or is contrary to law."

### A. The Governing Statutes Prohibit Unauthorized Access And The Stored Communications Act Provides For Statutory Damages For Each Violation

The Magistrate Judge's December 23 order is clearly erroneous and contrary to law because it prevents Plaintiffs from discovering when and how many times Defendant accessed Plaintiffs' email accounts and what he did with this information, which is information vital to determine the extent of Defendant's liability and Plaintiffs' damages. As Plaintiffs and their experts have repeatedly informed the Magistrate Judge, the production of the key word search results and the unallocated space does not provide the

necessary forensic information to determine when and how often Defendant accessed Plaintiffs' email accounts and what he did with this information.

An examination of the statutes at issue demonstrates why this information is vital to Plaintiffs' claims. As asserted in Count I, the CFAA prohibits the intentional ***accessing*** of a computer "without authorization or exceeding authorized ***access***" to obtain information from a "protected computer." 18 U.S.C. § 1030 (a)(2)(C) (emphasis added). Pursuant to Count II, Defendant is liable under the CFAA as one who: "knowingly and with intent to defraud, ***accesses*** a protected computer without authorization, or exceeds authorized ***access***, and by means of such conduct furthers the intended fraud and obtains anything of value. . . ." 18 U.S.C. § 1030(a)(4) (emphasis added).

Under Counts VI and VII, the SCA establishes liability against one who "intentionally ***accesses*** without authorization a facility through which an electronic communication service is provided" and "intentionally exceeds an authorization to ***access*** that facility; and thereby obtains, alters, or prevents authorized ***access*** to a wire or electronic communication while it is in electronic storage in such system." 18 USC § 2701(a)(1)&(2) (emphasis added). Thus, to establish liability under the CFAA and the SCA, Plaintiffs must be able to discover the occasions (other than the times of which they are already aware) on which Defendant accessed their e-mail accounts, as well as what he did with this information.

Defendant's use of the information (*e.g.*, in furtherance of an intended fraud as prohibited by the CFAA) is also relevant to Plaintiffs' damages under the CFAA and SCA. In addition, the SCA provides for $1,000 per-violation in statutory damages even where actual damages may be nominal. 18 U.S.C. § 2707(c); *see also In re the*

*Application of United States*, 441 F. Supp. 2d 816, 835 (S.D. Tex. 2006); *Voicenet Communs., Inc. v. Corbett*, 2006 U.S. Dist. LEXIS 61916 (E.D. Pa. Aug. 30, 2006); *In re Hawaiian Airlines, Inc.*, 355 B.R. 225 (D.Hawai'i 2006). Thus, the number of occasions Defendant accessed Plaintiffs' e-mail accounts without their authorization, and what he did with this information, is directly relevant to Plaintiffs' claims and damages, and Plaintiffs are entitled to discovery of these facts. As Plaintiffs' expert makes clear, this information cannot be obtained without a forensic analysis of Defendant's hard drive. A forensic analysis is also relevant to establish the grounds for the punitive damages Plaintiffs seek in this case because it will demonstrate Defendant's knowing, repeated violations of the SCA and CFAA.

**B. Plaintiffs' Expert Cannot Determine When And How Many Times Defendant Accessed Plaintiffs' Email Accounts Without Conducting A Complete Forensic Analysis Of Defendant's Imaged Hard Drive**

Plaintiffs' forensic expert, Jason Sprowl submitted four Declarations over the course of these two motions to compel explaining why a key word search cannot substitute for a complete forensic examination to determine when and how many times Defendant actually ***accessed*** Plaintiffs' email accounts and what he did with this information. Likewise, after Defendant extracted the unallocated space onto an external hard drive and produced it on December 4 along with the key word search results, Mr. Sprowl further explained that unallocated space extracted from Defendants hard-drive cannot simply be used in combination with the key words search results to determine when and how many times Defendant accessed Plaintiffs' email accounts. Defendant submitted two Declarations from his expert Benjamin Pim. For ease of reference,

Plaintiffs attach these four Plaintiff Declarations as Ex. P and the two Defendant declarations as Ex. Q.

During the briefing on the Second Motion to Compel, the fundamental dispute between Mr. Sprowl and Mr. Pim was whether the unallocated space and key word production was sufficient to conduct a forensic analysis which would enable Plaintiffs to determine how many times Defendant accessed Plaintiffs' email accounts. Mr. Sprowl stated repeatedly that Defendant's production of only key word results and the unallocated space extracted from Defendant's hard drive is incomplete and cannot answer the fundamental questions Plaintiffs seek to discover as to when and how many times Defendant accessed the email accounts and what he did with this information. Mr. Sprowl repeatedly explained that the key word results and unallocated space are a good start; however, they cannot replace the missing pieces of the whole forensic puzzle such as log files, temporary files, or deleted files which were not included in Defendant's production. Email artifacts can reside in several locations outside of unallocated space. Mr. Sprowl also explained this problem was especially acute on Defendant's MAC operating system (as opposed to Windows), where meta data can fork into several locations outside of unallocated space. The Magistrate Judge's December 23 Order denying Plaintiffs' Second Motion to Compel prevents Mr. Sprowl's forensic examination. It prevents him from being able to construct things such as time lines for Defendant's access times and prevents him from reconstructing Defendant's activity by dates. The Magistrate Judge's Order also prevents Mr. Sprowl from obtaining the hard-drive's log files and caches that Plaintiffs need for data related to e-mail activity. The chances of finding the log files needed to make these time line constructions and to trace

Defendant's access times are slim to none with the production solely of unallocated space and the key word search results. In same, the Magistrate Judge's Order impedes Plaintiffs' efforts to determine both Defendant's liability and Plaintiffs' damages under the SCA and CFAA.

In contrast to Mr. Sprowl's Declarations, Mr. Pim repeatedly bypasses the question of whether Defendant's production contains adequate meta data to determine Defendant's access times. Instead, he qualifies his statements to state that a forensic examination can take place within the parameters of the protocol ordered by the Magistrate Judge. In his first Declaration dated December 8, 2009, Mr. Pim states in paragraph 10 that "all relevant forensic data requested by the Plaintiffs ***under the protocol*** was produced in the native files and expert report produced on December 4, 2009." Mr. Pim's statement sets with a straw man argument because Plaintiffs were attacking the very efficacy of the Magistrate Judge's protocol Order to determine how many times Defendant accessed Plaintiffs' email accounts.

Mr. Pim's subsequent December 16, 2009 Declaration builds upon this argument. Tellingly, he does not state that the unallocated space and the files resulting from the key word results will contain all the meta data necessary to determine how many times Defendant accessed Plaintiffs' email accounts or what Defendant did with this information. Indeed, Mr. Pim does not dispute that there are many other locations other than unallocated space where meta data can reside, which could help identify Defendant's access times. Pim Dec. ¶ 6. Instead, Mr. Pim inaccurately indicates that Plaintiffs can discover anything they need from a combination of the unallocated space and the key word files. Yet, even Mr. Pim does not go so far as to declare that valuable

meta data necessary to determine Defendant's access Plaintiffs' email accounts cannot be found on other parts of the hard drive. As Mr. Pim should know, the unallocated space and the key word files that they produced are not nearly all of the relevant meta data contained on Defendant's hard drive. Still, Mr. Pim attempts to qualify his statements by claiming that the information ***should*** be available to Plaintiffs as long as Plaintiffs provided the correct key words. Pim Dec. ¶ 5. This simplistic approach ignores the large amount of data and missing log and temporary files that were not provided by the unallocated space or the key word results. Plaintiffs can not be expected to come up with perfect searches that will identify each time Defendant accessed Plaintiffs' email accounts – only Defendant possesses this information, but he refuses to produce it.

In summary, Plaintiffs repetedly provided the Magistrate Judge with expert testimony that makes clear that Defendant's provision of the result of the key word searches and the unallocated portion of Defendant's hard-drive will not tell Plaintiffs when and how many times Defendant accessed Plaintiffs' email accounts and what he did with this information. The Magistrate Judge erred by disregarding this expert testimony and the governing law. As demonstrated below, Courts almost always permit a plaintiff to conduct a complete forensic analysis in cases such as this one, and this case should be no exception.

### C. Defendant Has Admitted That He Repeatedly Accessed Plaintiffs' Email Accounts And Refused To Provide The Basis For The Attorney-Client Privilege That Is The Alleged Basis For Not Producing His Hard-Drive

Defendant has admitted that he accessed at least 4 of Plaintiffs' email accounts, and 1 such account for almost two years. *See* Ex. R at Interrogatory and Supplemental Interrogatory Responses Nos. 1-3, 5, 8. Yet, in his Rebuttal, Defendant concedes that he

has only produced two email strings, which not coincidentally are the same emails referenced in the Amended Complaint. (Ex. M at 3 & n.3). And, even though he claims to have a photographic memory (*See* Ex. S at 87-88), Defendant testifies that he simply cannot remember anything else he accessed and reviewed over a two year period of time. *See* Exhibit R at Interrogatory and Supplemental Interrogatory Responses Nos. 1-3, 5, 8. Thus, Defendant has only produced those materials that Plaintiffs specifically referred to when they brought this action and nothing more. Quite a coincidence.[2]

A forensic exam of Defendant's hard drive is regularly granted in cases involving the federal statutes at issue. *See, e.g., Physicians Interactive v. Lathian Systems, Inc.*, Case No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868 at *29-30 (E.D. Va. December 5, 2003) (permitting discovery of the hard drive, noting that "electronic evidence is at issue. Electronic evidence can easily be erased and manipulated."); *Koosharem Corp. v. SPEC Personnel, LLC*, Civ. No. 6:08-583, 2008 U.S. Dist. LEXIS 108396 at *4-6 (D.S.C. Sept. 29, 2008) (granting motion to compel computers for forensic analysis because, *inter alia*, such analysis could demonstrate accurate data regarding a communication that a mere print copy of the emails could not show); *Mintel Int'l Group, Ltd. v. Neergheen*, 2008 U.S. Dist. LEXIS 54119 (N.D. Ill. July 16, 2008) (in a case involving claims under 18 U.S.C. § 1030 and the Illinois Trade Secret Act, granting preliminary injunction and requiring defendant to produce forensic copies of all personal desktop and/or laptop computers); *Wolters Kluwer Fin. Servs. V. Scivantage*, 525 F.

[2] In order to independently determine what he accessed, Plaintiffs issued a subpoena to Go-Daddy. *(*Ex. T). Regrettably, its counsel advised Plaintiffs that Go-Daddy does not keep access logs for email accounts. (Ex. U). Thus, since Defendant refuses to tell Plaintiffs what he accessed, as Plaintiffs' expert Declarations make clear, the only possible way to determine what Defendant accessed is to forensically analyze the imaged-copy of his hard drive. *See* Ex. P.

Supp. 2d 448, 463 (S.D.N.Y 2007) (requiring production of computers and imaged copies of hard drives with respect to all computers implicated in claims asserted under, *inter alia*, 18 U.S.C. § 1030); *see also Orrell v. Motorcarparts of America*, Civ. No. 3:06CV418-R, 2007 U.S. Dist. LEXIS 89524 at *17 (W.D. N.C., Dec. 5, 2007) (granting motion to compel production of computers for forensic examination of hard drives where Court held that the party did not meet her burden of "do[ing] all she could under those circumstances to preserve evidence."). The *Orrell* Court noted that discovery under Rule 26 "including [discovery of] computer hard drives of the computers which generated emails that were later improperly deleted is proper and has been effected by other courts." *Id. at *18-19* (*citing Antioch Co. v. Scrapbook Borders, Inc*., 210 F.R.D. 645, 652 (D. Minn. 2002); *Simon Property Group L.P. v. MySimon, Inc*., 194 F.R.D. 639, 640 (S.D.N.Y. 2000); *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999)).

In order to not produce his hard drive, Defendant has repeatedly argued that to do so would be unfair in ***this*** case because it could require disclosure of attorney-client communications with his alleged clients. *See, e.g.*, Ex. M at 1, 4-5. The Magistrate Judge clearly fashioned the keyword search protocol based on Defendant's representations that the computer hard drive contained attorney-client communications. Indeed, at the October 23 hearing, the Magistrate Judge stated that "I wouldn't be doing it this way if it weren't a hard drive on which a substantial amount of material is, covered by the attorney/client privilege is stored." Defendant's attempt to claim attorney-client privilege is galling in light of Defendant's admission that he accessed and reviewed Plaintiffs' attorney-client communications and shared them with his attorney who was providing

legal advice regarding his divorce. *See* Ex. S at 9-12, 18 ; Ex. R, Interrogatory and Supplemental Interrogatory Responses at 1-3, 5, 8.

As importantly, at his deposition, Defendant admitted under oath that he has been "removed long enough from the daily practice of law" and refused to identify the name of a single client with whom he had an attorney-client privilege. *See* Ex. S at 16, 23-38. When pressed to do so in order to determine whether any attorney-client relationships actually existed that would support not producing Defendant's hard drive, Defendant's counsel instructed him not to answer the question. *Id.*[3] Defendant cannot continue to have it both ways – he cannot invoke the privilege to not produce his hard drive and then refuse to produce the most basic information in order to establish that a privilege exists in the first place.

Finally, Defendant's alleged concern also could be easily addressed by making those allegedly privileged communications subject to the Protective Order entered in this case (like Plaintiffs' attorney-client communications). As Plaintiffs offered before, these documents could even be classified as "attorneys' eyes only." As Plaintiffs have repeatedly stated, all they want is what Defendant accessed and what he did with that information – Plaintiffs have no interest in Defendant's attorney-client communications with his alleged clients about other matters. Plaintiffs also repeatedly offered the Magistrate Judge other solutions to accommodate these alleged attorney-client communications. In their Supplemental Brief in Support of the First Motion to Compel, Plaintiffs cited several cases which allowed plaintiff's expert to conduct an independent

[3] Defendant also testified that his law license had been suspended, but although he claims to have a photographic memory, he claims not to remember when it was suspended or for what time period. (Ex. S at 20-23). Obviously, there can be no privilege concerns for the period of Defendant's suspension.

forensic analysis, but then permitted defendant to conduct a privilege review prior to turning over the responsive information. In *Frees, Inc. v. McMillian*, No. 05-1979, 2007 U.S. Dist. LEXIS 4343, 2007 WL 184889, at *3 (W.D. La. Jan. 22, 2007), the plaintiff sued a former employee under the CFAA, (but not the SCA), for using the plaintiff's computers to remove the plaintiff's proprietary information while still employed by the plaintiff. 2007 U.S. Dist. LEXIS 4343, [WL] at *1. In granting the plaintiff's motion to compel the imaging and examination of the defendant's work and home computers, the court agreed with the plaintiff that the computers would be "among the most likely places [the defendant] would have downloaded or stored the data allegedly missing." 2007 U.S. Dist. LEXIS 4343, [WL] at *2. Although the defendant claimed he had acquired his computers two years after the misappropriation was alleged to have occurred, the Court found that even if that were true, the computer could still contain evidence related to the "pilfered" data. *Id.* To address privilege, privacy and confidentiality concerns, the Court created a protocol that allowed the defendant to review the imaged copy of the hard-drive to ensure that privileged or non-responsive information would not be produced and, after the defendant's review, the plaintiff's expert would then be permitted to examine the image to identify relevant files for production. Once the expert identified those files, the defendant would have a chance to object to the production of any file on grounds such as privilege. 2007 U.S. Dist. LEXIS 4343, [WL] at *3.

In *Ameriwood Indus., Inc. v. Liberman*, No. 4:06 CV 524-DJS, 2006 U.S. Dist. LEXIS 93380, 2006 WL 3825291, at *3, *6 (E.D. Mo. Dec. 27, 2006), amended by 2007 U.S. Dist. LEXIS 10791, 2006 WL 685623 (E.D. Mo. Feb. 13, 2007), the plaintiff sued several former employees and their newly formed company under, *inter alia*, 18 U.S.C. §

1030, for unlawfully using the plaintiff's computers to remove proprietary information and trade secrets to "sabotage [the] plaintiff's business relationships and divert [the] plaintiff's business to themselves." Specifically, the plaintiff alleged that the defendants had forwarded trade secrets to their personal e-mail accounts while employed by the plaintiff. *Id*. The defendants objected to this request as "overbroad, vague, burdensome, and call[ing] for irrelevant information." *Id*. at *2. The defendants also argued that they had already searched for and disclosed responsive information from their hard drives. *Id.* at *3. The court noted, however, that some electronically stored information "***might not be obtained during a typical search" of the hard drives***. *Id*. (emphasis added.)

The court explained that, "in cases where a defendant allegedly used the computer itself to commit the wrong that is the subject of the lawsuit, certain items on the hard drive may be discoverable," and that "allegations that a defendant downloaded trade secrets onto a computer provide a sufficient nexus between plaintiff's claims and the need to obtain a mirror image of the computer's hard drive." *Id*. at *4. Because the plaintiff alleged that the defendants had used their computers to distribute the plaintiff's confidential information, ***"[h]ow and whether [the] defendants handled those documents and what [the] defendants did with the documents is certainly at issue***." *Id*. at *5 (emphasis added). Thus, the court allowed "an independent expert to obtain and search a mirror image" of the defendants' computers, given the "close relationship" between those computers and the plaintiff's claims, as well as the court's doubts that the defendants had produced all responsive documents. *Id*. at *1.

Nonetheless, recognizing privacy concerns, the court adopted a three-step procedure for disclosure: (1) an independent expert, bound by a confidentiality

agreement, make a mirror image of and recover all files from the defendants' hard drives; (2) the expert then provides all recovered files and information about those files (such as information as to when those files were created, accessed, copied, or deleted) to the defendants' counsel; and (3) within 20 days of the receipt of the recovered files, the defendants produce any non-privileged and responsive documents to the plaintiff. *Id*. at *5-6; *see also Cenveo Corp. v. Slater*, No. 06-CV-2632, 2007 U.S. Dist. LEXIS 8281, 2007 WL 442387, at *1-3 (E.D. Pa. Jan. 31, 2007) (citing *Ameriwood* and adopting similar procedure).

The same compelling grounds that warranted production of the computer in *Frees, Ameriwood,* and the other cases cited above apply to this case; however, the Magistrate Judge erred by not ordering the production of Defendant's computer. Plaintiffs proposed virtually the same protocol for disclosure as was implemented in these cases, to protect Defendant's alleged privacy interest. That is, Plaintiffs proposed that their expert agree to the Protective Order, perform the forensic analysis on the imaged hard drive necessary in his expert opinion to reveal the relevant information, and then hand over the relevant information, document and files to counsel for Defendant. Defendant's counsel then could review the files for privilege, create a privilege log, and produce the privilege log, along with all non-privileged, responsive documents.

## IV. CONCLUSION

For the forgoing reasons, Plaintiffs' ask the Court to sustain these Objections to the Magistrate Judge's December 23, 2009 Order. Order Defendant to produce the imaged-copy of his computer hard-drive to Plaintiffs so they may conduct a complete forensic examination, and adjust the expert deadlines.

**Dated: December 31, 2009**

**Respectfully Submitted,**

**PLAINTIFFS**
By Counsel

/s/

Stephen J. Stine, Esq.
Virginia State Bar. #66738
Bernard J. DiMuro, Esq.
Virginia State Bar # 18784
Stephen L. Neal, Jr., Esq.
(*pro hac vice*)
Stacey Rose Harris, Esq.
Virginia State Bar #65887
*Counsel for Plaintiffs*
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: (703) 684-4333
Fax: (703) 548-3181
E-Mails: sstine@dimuro.com;
bdimuro@dimuro.com;
sneal@dimuro.com;
sharris@dimuro.com.

**CERTIFICATE OF SERVICE**

I hereby certify that on this 31st day of December, 2009, I electronically filed the foregoing brief with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following counsel of record:

Charles M. Sims, Esq.
*Counsel for Defendants*
LeClairRyan
951 East Byrd Street, 8th Floor
Richmond, VA 23219
Phone: (804) 343-5091
Fax: (804) 783-7655
Email: charles.sims@leclairryan.com;

C. Matthew Haynes, Esq.
*Counsel for Defendants*
LeClairRyan
2318 Mill Road, Suite 1100
Alexandria, VA 22314
Phone: (703) 684.8007
Fax: (703) 684- 8075
Email: matthew.haynes@leclair.com

/s/
Stephen J. Stine, Esq.
Virginia State Bar. #66738
Bernard J. DiMuro, Esq.
Virginia State Bar # 18784
Stephen L. Neal, Jr., Esq.
(*pro hac vice*)
Stacey Rose Harris, Esq.
Virginia State Bar #65887
*Counsel for Plaintiffs*
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: (703) 684-4333
Fax: (703) 548-3181
E-Mails: sstine@dimuro.com;
bdimuro@dimuro.com;
sneal@dimuro.com;
sharris@dimuro.com.